NORFOLK STATE UNIVERSITY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2021

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We have audited the basic financial statements of Norfolk State University (the University) as of and for the year ended June 30, 2021, and issued our report thereon, dated May 9, 2022. Our report, included in the University's Annual Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the University's website at www.nsu.edu. Our audit found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and
- instances of noncompliance or other matters required to be reported under Government Auditing Standards.

Our audit also included testing over the major federal programs of the Student Financial Assistance Programs Cluster and Education Stabilization Fund for the Commonwealth's Single Audit as described in the U.S. Office of Management and Budget Compliance Supplement; and identified three internal control findings requiring management's attention and instances of noncompliance in relation to this testing.

–TABLE OF CONTENTS–

	Pages
AUDIT SUMMARY	
STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS	1-6
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	7
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	8-10
UNIVERSITY RESPONSE	11-14
UNIVERSITY OFFICIALS	15

STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS

Continue to Improve Information Security and Risk Management and Contingency Programs
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2016, with limited progress in this area)

The University does not manage certain aspects of its Information Technology (IT) Risk Management and Contingency Program in accordance with the Commonwealth's Information Security Standard, SEC 501 (Security Standard) and University policy. The IT risk management and contingency program provides the baseline for the University to recover and restore mission-critical and sensitive systems based on the University's identification, assessment, and management of information security risks. The University is making progress to improve and update its IT risk management and contingency program and process by completing its business impact analysis (BIA), system inventory and definition plans, and system security plans. However, the following control weaknesses exist:

- The University has 15 sensitive systems that require a risk assessment. The University does not have risk assessments for 11 of the 15 systems. The University completed risk assessments for four of the 15 systems but did not perform an annual review and revision for three of the four completed risk assessments requiring an annual review. Without conducting a risk assessment for each sensitive system, management may not correctly prioritize information security risks and implement appropriate controls to help mitigate those risks. By not updating its risk assessments to reflect changes to its sensitive systems, the University increases the risk of not securing its sensitive systems adequately against known vulnerabilities that can affect data confidentiality, integrity, and availability. (*Administrative Policy 32-8-6 Risk Assessment; Security Standard: 6 Risk Assessment)*

- The University does not have a disaster recovery plan (DRP) detailing how the University will manage a disruptive event to restore its mission critical systems within the recovery point objectives (RPOs) and recovery time objectives (RTOs). Additionally, the University does not perform annual DRP testing and has no schedule to conduct DRP tests. The University documented a draft version of the DRP in February 2022 but has not yet completed the DRP. Without completing a DRP that prescribes the process to restore mission critical systems and without performing disaster recovery tests to determine restoration processes function effectively, the University increases the risk that in the event of a disaster, it may not be able to recover sensitive and mission critical systems in a timely manner. DRP testing is essential to ensure the appropriate processes exist and work effectively without disrupting operations in order to restore a system and its application(s) to full functionality in the event of a system failure or disaster. *(Security Standard: CP-1-COV Contingency Planning Policy and Procedures; and CP-4 Contingency Plan Testing and Exercise)*

- The University does not use the expected time frames to restore specific business functions outlined in the BIA to determine RTOs and RPOs for specific IT systems in the DRP. The Security Standard requires the University to use the information in the BIA to develop components of the DRP, including RTOs and RPOs to restore to normal operations, and to verify consistency between the artifacts. Without outlining in the DRP which RTOs and RPOs to follow for each IT system, the University may not appropriately restore the systems necessary to recover business operations. (*Security Standard: CP-1-COV-1 Contingency Planning Policy and Procedures*)

Turnover and a lack of resources led to the University having an incomplete risk management and contingency planning program. Risk management and contingency planning has been an ongoing concern and originally identified in our audit for fiscal year 2016. Since 2016, the University has obtained information security officer (ISO) services from the Virginia Information Technologies Agency (VITA) to assist them in the process of developing their IT risk management and contingency planning documentation and, although these services have not progressed as planned, the University continues to work with VITA to complete a comprehensive risk management and contingency planning program.

The University should continue to implement its corrective action plan to develop and maintain an information security program that meets the requirements in the Security Standard. Specifically, the University should develop a plan with VITA to expedite the completion of all outstanding risk assessments and ensure that VITA completes the risk assessments as planned. Further, the University should dedicate the necessary resources to prioritize the development and implementation of its IT continuity of operations plan and complete and approve the IT DRP. Finally, the University should perform annual disaster recovery testing. Developing and maintaining effective and consistent IT risk management and contingency planning documentation will help to ensure that the University can adequately protect sensitive systems and data and bring systems online in a timely manner to resume normal business operations in the event of an emergency or disaster.

Continue to Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act (GLBA)
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2020)
Prior Title: Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act

The University does not implement all cybersecurity requirements of the Gramm-Leach-Bliley Act (GLBA) and University policy. Specifically, the University completed a risk assessment for four of 15 sensitive systems but does not have risk assessments for the remaining 11 sensitive systems. Additionally, the University has not evaluated each of its systems to determine which systems contain customer information specifically protected under the GLBA.

Federal regulations consider institutions of higher education, because of their engagement in financial assistance programs, to be financial institutions that must comply with Public Law 106-102, known as the GLBA. Related regulations within the 16 U.S. Code of Federal Regulations (CFR) 314.4, require organizations to develop, implement, and maintain information security programs to safeguard

customer information and complete a risk assessment that includes consideration of risks in each relevant area of operation. Additionally, the University's risk assessment policy requires conducting and documenting a risk assessment for each IT system classified as sensitive.

Without implementing cybersecurity requirements of the GLBA for each system containing non-public customer information, the University may not be able to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to the University's customers.

The University procured VITA's ISO services to assist in completing risk assessment reports. However, VITA's ISO services have not been able to complete the University's risk assessment reports as planned. During this period, the University did not explore alternative avenues to complete its risk assessments in a timely manner.

The University should evaluate its systems to determine which systems contain customer information, then document and complete a risk assessment for each system on the list. If current internal or procured resources cannot complete this task in a timely manner, the University should explore new avenues to assist in completing these important information security documents. Conducting a risk assessment for each system containing non-public customer information will aid in protecting customer information and meet the requirements set forth in the GLBA.

Continue to Upgrade End-of-Life Technology

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2015, with limited progress in this area)
Prior Title: Continue to Upgrade or Decommission End-of-Life Technology

The University continues to use end-of-life technologies in its IT environment. The University is making progress to upgrade, replace, or decommission the unsupported technologies; however, the University maintains technologies that support mission-essential data on IT systems running software that its vendor no longer supports.

We communicated the control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under §2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Commonwealth's Security Standard prohibits agencies from using software that is end-of-life and which the vendor no longer supports, to reduce unnecessary risk to the confidentiality, integrity, and availability of the University's information systems and data.

The University should dedicate the necessary resources to evaluate and implement the controls and recommendations discussed in the communication marked FOIAE in accordance with the Security Standard. Implementing corrective action will help to ensure that the University secures its IT environment and systems to protect its sensitive and mission-critical data.

Remove System Access Timely
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2019)
Prior Title: Improve Controls over Purchasing System Access

The University did not deactivate terminated employees' access to the Commonwealth's purchasing system or the University's network in a timely manner. The University did not begin the deactivation process within 24 hours after separation for seven out of 11 (64%) terminated employees with access to the purchasing system, and for seven out of nine (78%) terminated employees with access to the University's network during fiscal year 2021.

The Commonwealth's Security Standard, Section PS-4a, requires that an organization disable information system access within 24 hours of employment termination. Additionally, the Commonwealth's purchasing system security standard, Section 2.10, states that in cases involving personnel issues such as termination, those employees with purchasing system access shall be reported immediately to the entity's Security Officer so action can be taken to deactivate access as needed. The University's logical access control policy and purchasing system user access policy requires system access be removed and account deactivation within 24 hours of notification of employment termination. Untimely removal of user access increases the risk of unauthorized transactions that can compromise the integrity of the University's and Commonwealth's systems.

Due to the decentralized nature of the University's operations, individual departments are required to report terminations to start the access removal process. When departments do not report terminations timely or accurately, the Office of Information Technology and security officers cannot process deactivations timely. Although the deactivation process began within 24 hours of notification of termination, the initial notifications occurred between three and 480 days after termination. The University should ensure that department report employment terminations timely, so that the University can deactivate user accounts belonging to terminated employees in accordance with the University's and Security Standard's requirement of 24 hours.

Comply With Prompt Payment Provisions
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)

During fiscal year 2021, the University did not process payments in compliance with the prompt payment requirements of the Virginia Public Procurement Act (VPPA). In our sample of 28 vouchers for which prompt payment requirements were applicable, we identified six instances (21%) in which the University did not process payment within the required 30 days.

Section 2.2-4350 of the Code of Virginia requires state agencies to pay for delivered goods and services within 30 calendar days after receipt of a proper invoice, or 30 days after receipt of the goods or services, whichever is later. Not following prompt payment requirements established by the Code of

Virginia may harm the University's reputation as a buyer, damage relationships with vendors, and could result in late fees.

Late payments were primarily the result of delays by individual departments in updating purchase orders or informing the Accounts Payable Department of payment authorization on invoices. Without an accurate and properly approved purchase order or an authorization of payment from the purchasing department, the Accounts Payable Department cannot process payment for the respective vendor charges.

The University should ensure proper processing of all vendor payments in compliance with the prompt payment requirements of the VPPA. To support compliance, the University should improve processes to ensure that departments approve and submit required documentation in a timely manner to the Accounts Payable Department to ensure it properly pays invoices within the 30-day period.

Improve Compliance over Enrollment Reporting
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Improve Reporting to National Student Loan Data System

The University's Registrar's Office personnel did not report accurate and timely enrollment data to the National Student Loan Data System (NSLDS) for students that had graduated, withdrawn, or had another applicable enrollment level change. The underlying cause of the errors is a combination of factors including late batches, the University reporting students as withdrawn rather than graduated for fall 2020, batch overwrites, and other concerns that the University will have to research with its third-party servicer. From a review of 50 students, we identified the following deficiencies:

- Inaccurate enrollment statuses for 15 students (30%);
- Inaccurate effective dates for 32 students (64%);
- Untimely reporting of enrollment changes for 49 students (98%); and
- Inaccurate reporting of at least one critical campus or program-level field for 33 students (66%).

In accordance with 34 CFR 685.309 and the NSLDS Enrollment Guide, published by the Department of Education (ED), enrollment changes must be reported to NSLDS within 30 days when attendance changes, unless a roster file will be submitted within 60 days. Not properly and accurately reporting a student's enrollment status may interfere with establishing a student's loan status, deferment privileges, and grace periods. In addition, the accuracy of the data reported by each institution is vital to ensuring that federal Direct Loan records and other federal student records remain updated.

The University should evaluate its current enrollment reporting procedures. Management should implement corrective measures to prevent future noncompliance. Where applicable, management should also consider implementing a quality control review process to monitor the accuracy of campus and program-level batch submissions.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Properly Process Return of Title IV Calculations
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The University's Office of Financial Aid did not consistently perform accurate return of Title IV calculations when disbursing Federal Supplemental Educational Opportunity Grants (FSEOG) during aid year 2021 because the University did not correctly code the FSEOG matching requirement within the student information system. Due to the University inaccurately coding the matching requirement, the calculation used 75 percent of each applicable student's FSEOG disbursement instead of 100 percent. As a result, for four out of 25 (16%) students reviewed, the University should have returned a total of $487 additional unearned funds to ED.

In accordance with 34 CFR 668.22, when a recipient of a Title IV grant or loan assistance withdraws from an institution during a period of enrollment in which the recipient began attendance, the institution must determine the amount of Title IV grant or loan assistance that the student earned as of the student's withdrawal date and return the unearned amount within a reasonable timeframe. An institution must use the full amount of FSEOG if ED supplied the entirety of the FSEOG funds. The University has a waiver from the FSEOG matching requirement, and as such, ED provides the full amount of FSEOG grants. The University should configure its system to accurately calculate the return of Title IV funds using 100 percent of a student's FSEOG disbursement.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

May 9, 2022

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
Norfolk State University

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the business-type activities and aggregate discretely presented component units of **Norfolk State University** (the University) as of and for the year ended June 30, 2021, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated May 9, 2022. Our report includes a reference to other auditors. We did not consider internal controls over financial reporting or test compliance with certain provisions of laws, regulations, contracts, and grant agreements for the financial statements of the University's component units, which were audited by other auditors in accordance with auditing standards generally accepted in the United States of America, but not in accordance with Government Auditing Standards.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's

internal control. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Continue to Improve Information Security and Risk Management and Contingency Programs," "Continue to Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act (GLBA)," "Continue to Upgrade End-of-Life Technology," "Remove System Access Timely," "Comply With Prompt Payment Provisions," "Improve Compliance over Enrollment Reporting," and "Properly Process Return of Title IV Calculations," which are described in the sections titled "Status of Prior Year Findings and Recommendations" and "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the sections titled "Status of Prior Year Findings and Recommendations" and "Internal Control and Compliance Findings and Recommendations" in the findings and recommendations titled "Continue to Improve Information Security and Risk Management and Contingency Programs," "Continue to Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act (GLBA)," "Continue to Upgrade End-of-Life Technology," "Remove System Access Timely," "Comply With Prompt Payment Provisions," "Improve Compliance over Enrollment Reporting," and "Properly Process Return of Title IV Calculations."

The University's Response to Findings and Recommendations

We discussed this report with management at an exit conference held on May 5, 2022. The University's response to the findings and recommendations identified in our audit is described in the accompanying section titled "University Response." The University's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Status of Prior Findings and Recommendations

The University has not taken adequate corrective action with respect to the previously reported findings and recommendations "Continue to Improve Information Security and Risk Management and Contingency Programs," "Continue to Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act (GLBA)," "Continue to Upgrade End-of-Life Technology," "Remove System Access Timely," "Comply With Prompt Payment Provisions," and "Improve Compliance over Enrollment Reporting." Accordingly, we included these findings and recommendations in the section titled "Status of Prior Year Findings and Recommendations." The University has taken adequate corrective action with respect to audit findings and recommendations reported in the prior year that are not repeated in this report.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

DLR/vks

NORFOLK STATE UNIVERSITY
We see the future in you.

FINANCE AND ADMINISTRATION
700 Park Ave., HBW Suite 310, Norfolk, Virginia 23504
P: 757-823-8011 | F. 757-823-8084 | nsu.edu

May 9, 2022

Ms. Stacie Henshaw
The Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218-1295

Dear Ms. Henshaw:

Norfolk State University has reviewed the Internal Control and Compliance Findings and Recommendations provided by the Auditor of Public Accounts for the fiscal year ending June 30, 2021, and agrees in principle with all of the findings.

Attached for your consideration is a brief update as to where the University is with respect to the findings. The formal Corrective Action Workplan will be submitted within thirty days as required by the CAPP Manual Topic No. 10205. However, if you have any questions or require additional information, please contact Ms. Karla Amaya Gordon, AVP for Finance and Administration/University Controller, 757-623-8345, kjagordon@nsu.edu; or me.

On behalf of Norfolk State University, please extend our appreciation to all of your staff for their professional audit work and recommendations.

Sincerely,

Gerald E. Hunter, PhD
Vice President for Finance and Administration

Cc: Javaune Adams-Gaston, PhD, President
Justin Moses, JD, EdD, VP for Operations & Chief Strategist for Institutional Effectiveness
Karla Amaya Gordon, AVP for Finance and Administration/University Controller
Derika Burgess, University Internal Auditor
S. Faye Monroe-Davis, Chief Information Officer
Ruby Spicer, Director of Procurement Services
Juan Alexander, PhD, AVP for Enrollment Management
Melissa Barnes, Director of Financial Aid

NORFOLK STATE UNIVERSITY
We see the future in you.

FINANCE AND ADMINISTRATION
700 Park Ave., HBW Suite 310, Norfolk, Virginia 23504
P: 757-823-8011 | F. 757-823-8084 | nsu.edu

FY 2021 – Internal Control & Compliance Findings
Management Response

Continue to Improve Information Security, Risk Management and Contingency Programs
As noted in last year's 2020 audit, NSU initiated and carried out a Risk Assessment process to identify, document and assess new and existing applications. NSU completed Risk Management activities including System Security Plans for all 15 NSU sensitive systems. The activities were completed prior to December 2021.

NSU receives ISO services from VITA that include development of the documentation required to complete each of NSU's 15 sensitive system assessments. The contracted services have not progressed as planned, resulting in 11 incomplete risk assessments. The University has implemented a corrective action plan with VITA to expedite the completion of all the outstanding Risk Assessments (RAs) as contracted. NSU will seek alternative options to complete the risk assessments as a function of our newly acquired Level II autonomy, if VITA fails to meet the agreed upon milestones in the corrective action plan.

Disaster Recovery - NSU completed a draft of the OIT Disaster Recovery Plan in February 2022. The draft requires a major overhaul, which was provided when interviewed as part of the audit process.

NSU understands the importance of DRP testing and will develop a test schedule once the OIT DRP is finalized. Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) have been created as a product of the Business Impact Analyses conducted in 2021 and will be included in the completed DRP. NSU has been actively meeting to complete the OIT DRP since mid-2021.

Implement Cybersecurity Requirements of the Gramm-Leach-Bliley Act
Given that GLBA requirements have changed, NSU will become familiar with the new GLBA tenets and develop and implement a plan that identifies systems containing non-public customer financial data. Once the systems are identified, NSU will develop policies and procedures that ensure compliance with the updated GLBA requirements.

Continue to Upgrade or Decommission End-of Life Technology
NSU has been working diligently to upgrade, replace or decommission all unsupported software. NSU plans to complete the remaining systems (12%) before the end of the calendar year. None of the remaining unsupported systems are mission essential.

NORFOLK STATE UNIVERSITY
We see the future in you.

FINANCE AND ADMINISTRATION
700 Park Ave., HBW Suite 310, Norfolk, Virginia 23504
P: 757-823-8011 | F. 757-823-8084 | nsu.edu

FY 2021 – Internal Control & Compliance Findings
Management Response (Cont'd)

Remove System Access Timely
The University is developing a workgroup to address the timeliness of departments completing the employee clearance process to ensure timely removal of system access. Additionally, the University will review and make necessary policy and procedure updates to ensure compliance with established standards.

Comply with Prompt Payment Provisions
The University will review the policy and procedures and make necessary updates to ensure compliance with the prompt payment requirement. Additionally, the University will provide divisional training for budget managers and fiscal staff on the importance of timely receipts of goods and services within the University's financial system and providing Accounts Payable the appropriate authorization time to pay invoices.

Improve Compliance over Enrollment Reporting
The NSU Registrar's Office has implemented the following enrollment reporting process into the Enrollment Verification Policies and Procedures to ensure that accurate data is submitted to the National Student Clearinghouse:

1. After every batch for student who graduated, the Registrar staff check the National Student Clearinghouse every five days to ensure that all graduation information reported is accurate.
2. When graduating students after the first graduation batch is processed, any student who is conferred after will be manually processed in the National Student Clearinghouse database instead of batch processing those individuals. The Registrar staff will ensure that graduation statuses are checked at least twice after the initial reporting.
3. The Office of the Registrar will ensure that all graduates for the preceding semester are processed before the next semester batch is run for the preceding semester.
4. The Office of the Registrar will closely with the National Student Clearinghouse to ensure that all data reported is accurate and timely in the case of campus or program level fields.
5. For students who officially withdraw from the University, the Registrar staff will send submission of students records to ensure that the enrollment status is not overwritten in subsequent batches for the current semester.
6. For students who unofficially withdraw from the University, the Registrar staff will manually review the enrollment status at least twice to ensure that the enrollment status is not overwritten in subsequent batches for the current semester.
7. The University Registrar will oversee the processing of enrollment verification for the next reporting cycle.

NORFOLK STATE UNIVERSITY
We see the future in you.

FINANCE AND ADMINISTRATION
700 Park Ave., HBW Suite 310, Norfolk, Virginia 23504
P: 757-823-8011 | F. 757-823-8084 | nsu.edu

FY 2021 – Internal Control & Compliance Findings
Management Response (Cont'd)

Properly Process Return to Title IV (R2T4) Calculations

The NSU Financial Aid staff updated the system to reflect a code of N (No) for FSEOG and 75% Federal Funds field and recalculated all students who were awarded federal SEOG that withdrew during the 2020-21 academic year. The Financial Aid Office also recalculated R2T4 for all students who were awarded FSEOG and who withdrew during the fall 2020, spring 2021 and summer 2021 semesters. All Pell and Direct Loans records have been corrected via the U.S. Department of Education's Common Originations and Disbursements (COD).

NORFOLK STATE UNIVERSITY

As of June 30, 2021

BOARD OF VISITORS

Devon M. Henry, Rector

Mary L. Blunt, Vice Rector

Kim W. Brown, Secretary

Heidi W. Abbott	BK Fulton
Terri L. Best	Larry A. Griffith
Dwayne B. Blake	Delbert Parks
Deborah M. DiCroce	Harold L. Watkins, II
James W. Dyke, Jr.	Joan G. Wilmer

UNIVERSITY OFFICIALS

Javaune Adams-Gaston, President

Gerald E. Hunter, Vice President for Finance and Administration